DOCUMENT RESUME

ED 314 069 IR 053 003

AUTHOR Johnson, David R.; And Others
TITLE Computer Viruses. Legal and Policy Issues Facing Colleges and Universities.
INSTITUTION American Council on Education, Washington, D.C.; United Educators Insurance, Chevy Chase, MD.
PUB DATE May 89
NOTE 17p.
PUB TYPE Legal/Legislative/Regulatory Materials (090) -- Viewpoints (120)

EDRS PRICE MF01/PC01 Plus Postage.
DESCRIPTORS Administrative Policy; College Faculty; *Colleges; *Computer Networks; *Computer Software; Contracts; Higher Education; *Legal Problems; Microcomputers; Student Behavior; Telecommunications; Torts
IDENTIFIERS *Computer Crimes; *Computer Viruses

ABSTRACT

Compiled by various members of the higher educational community together with risk managers, computer center managers, and computer industry experts, this report recommends establishing policies on an institutional level to protect colleges and universities from computer viruses and the accompanying liability. Various aspects of the topic are addressed, including: (1) what a computer virus is, how it is spread, how it can be detected, the kind of damage it can do, how viruses are created and launched, what makes colleges and universities especially at risk, and available technical protective measures; (2) the legal issues, including criminal statutes, tort liability (i.e., the university's liability for student conduct and its role as employer), contractual implications, and statutory duties related to privacy; and (3) specific priorities and options, such as establishing policies for student and faculty conduct, distribution of information about viruses throughout the campus, limiting access to college computers, establishing operational safeguards, creating an emergency action plan, and developing plans for responding to governmental inquiries. A review of contractual rights and obligations and suggestions for dealing with specific problems are included. (SD)

United Educators
Insurance Risk Retention
Group, Inc.

Two Wisconsin Circle, Suite 1040
Chevy Chase, Maryland 20815-9913
(301) 907-4908 (800) 346-7877

AMERICAN COUNCIL ON EDUCATION

Division of Governmental Relations

One Dupont Circle, Washington, D.C. 20036-1193 (202) 939-93

May 1989

Computer Viruses

Legal and Policy Issues

Facing Colleges and Universities

This paper was produced jointly by United Educators Insurance and the American Council on Education and was written by David R. Johnson, Thomas P. Olson and David G. Post of Wilmer, Cutler & Pickering, Washington, DC. The comments and contributions of various members of the higher education community in Washington are appreciated, along with the work of a good many university counsel, risk managers, computer center managers and industry experts whose comments and suggestions contributed significantly to the finished product. Special thanks to Sheldon E. Steinbach, Vice President and General Counsel of the American Council on Education, who shepherded this project through to its completion.

Now that the first wave of publicity (and some hysteria) has passed, it is time for colleges and universities to reflect on the legal and policy issues raised by the threat of computer viruses. As usual, there is no simple answer to these questions -- no one right policy that every college ought to adopt. But the threats are serious enough that all colleges will want to spend time considering the key issues and adopting a set of policies appropriate for their own circumstances. This White Paper is designed to aid in that exercise.

Executive Summary

A computer virus may disrupt campus computers or, launched from a campus into the outside world, may cause serious harm to others. Intentionally launching a virus is a serious crime. A college or university that fails to take reasonable steps to avoid the use of its facilities to perpetrate such an offense might face claims that it is liable under tort law for the resulting damage. A college should consider the possibility of such liability in its contractual dealings with third parties. In addition, a college should carefully consider adopting policies and procedures that will reduce the risk of harm from computer viruses, consistently with other educational and institutional goals, such as distributing information on how to protect against a computer virus attack, establishing reasonable limitations on access to college computers, establishing operational safeguards to be implemented by trained computer professionals, and creation of emergency action plans.

I. Background Facts

A. What is a Computer Virus?

A computer virus, as the term is generally used, is a computer program that can cause copies of itself (or parts of itself) to be created. A computer virus may be found within another, apparently harmless, computer program or it may be a separate program that simply produces other copies of itself (this kind of program might be called a "worm"). The copies created by a computer virus may invade other programs or preexisting files or may be stored in separate files on the disks of computers to which the virus has

access. Different types of computer viruses, which act in slightly different ways, might be called "pests", "Trojan horses", or "logic bombs" (these categories may also refer to programs that cause disruption but, strictly speaking, do not replicate themselves). Their generally shared characteristics are that they operate in ways that would not be approved by the user, may spread by deception from computer system to computer system, are difficult to control and can create significant harm.

B. How Can a Computer Virus Spread?

A computer virus can spread to a new computer system whenever the computer program in which it is included is connected -- directly or indirectly -- to a new computer or computer disk. Thus, a particular virus may be propagated through the telephone lines or cables connecting computers in an on-campus network. Or it may be transmitted from disk to disk as copies of programs or data are physically transferred among different machines.

C. How Can a Computer Virus Be Detected?

It is not always easy to tell whether a particular disk or computer program has been infected with a computer virus. Indeed, some viruses may be designed as "time bombs" to be activated at particular times or after specific events occur. As a result, a virus can be widespread before any disruptive effects become apparent.

Most often, a virus is detected as a result of some malfunction that it causes in a computer system. On the other hand, most computer malfunctions are NOT due to viruses. Experts who carefully inspect a system will often be able to determine whether it harbors a computer virus. Since a virus must write files or alter programs in memory to cause itself to be copied, some screening programs are available to watch for such activity and to provide early alerts that particular types of viruses are present. These detection programs work most effectively with viruses that act in a predictable fashion or have been studied for some time.

D. What Kind of Damage Can a Computer Virus Do?

A computer virus can cause substantial harm simply by replicating itself many times and using up disk space and computing power in a computer system. In addition, a virus could well delete or damage other computer files. Depending on the nature of the adversely affected computer program or file, substantial damage may be done to a wide range of different interests. Perhaps the most common type of harm, however, is the burden of cleaning up the system – removing, checking, and replacing files. The technical services required to remove a virus may be very expensive. Missing even a single copy of a virus may cause the problem to recur.

E. How Difficult is it to Create and Launch a Computer Virus?

Although the press tends to characterize those who have launched viruses as rare geniuses, it does not take an extraordinary level of programming expertise to create a program that will cause itself to be copied and that could do harm to other computer systems. The threat does not stem solely from programs created on campus, in any event. Even if no one at a particular college has any intention of sabotaging its computer systems, the introduction of a virus into a campus computer system may occur through the use or copying of a file by a student or faculty member who does not realize the risk posed by the program (the modern day equivalent of a "Typhoid Mary").

F. Are Colleges and Universities Especially at Risk?

Probably. Institutions of higher learning often have an unusual concentration of people with computer expertise and the freedom and incentive to explore frontier technologies. Unfortunately, the creation of computer viruses has developed a reputation as a challenging and intellectually intriguing activity. In addition, students and faculty often copy and exchange computer software, including software that has not gone through regular commercial channels, as to which the risk of computer virus infection is greatest. Moreover, much college and university computing takes place in the context of computer centers and large networks, which can offer ideal

conditions for the spread of computer viruses.

G. Are Technical Protective Measures Available?

No absolute protection is available. But some technical steps can be taken to reduce the risk of harm and, correspondingly, the risk of liability for harm caused to others. (Some of those steps are discussed in more detail below). On the other hand, some actions that might maximize protection against a computer virus could also interfere drastically with productive use of computers by students, staff, and faculty. Thoughtful consideration of the relevant tradeoffs, and implementation of policies appropriate to your institution, will pay off.

II. Overview of Legal Issues

While every college or university should design and implement policies that reflect its unique circumstances, each must take into account a similar set of legal issues.

A. Criminal Statutes.

It is a serious crime to launch a computer virus, intentionally, by means of entering a computer system without authority, or intentionally to destroy or deny authorized access to computer systems. In general, the crime is one under Federal law if the computer system is used substantially for U.S. Government purposes (or by a financial institution). See Computer Fraud and Abuse Act. The crime may also be a Federal one if launching the virus involved obtaining unauthorized access to an electronic communications system affecting interstate commerce. See Electronic Communications Privacy Act. Almost all states also have laws that make it a crime intentionally to damage or disrupt computer systems, whether through the use of a computer virus or otherwise. Additional legislation targeting the threat of computer viruses is pending in various jurisdictions. (E.g., Computer Virus Eradication Act of 1988, introduced as HR 5061). Although existing law is generally adequate to condemn such activity, serious problems of proof -- such as establishing the source of the virus and explaining to a

court the complex technical issues involved -- remain. Many such incidents might not be successfully prosecuted.

B. Tort Liability.

Someone damaged by a computer virus may seek to recover compensation in a civil lawsuit -- and may seek a defendant with "deep pockets". In view of the wide range of activities in which a modern university or college computer center may be involved, it is, unfortunately, not difficult to imagine the kinds of damage claims that may be asserted if a virus causes widespread destruction of computer files:

• a financial institution, off campus, could lose key records and suffer serious harm from a widely distributed virus, and may feel compelled to assert a claim against the institution in whose facilities the virus originated;

• a virus in an on-campus hospital could destroy or alter medical records, potentially causing serious harm to patients.

• a consulting firm working with a faculty member may seek to recover the value of revenues lost because of a default caused by a disruptive on-campus virus;

To the extent a virus travels along a network to other facilities, the risk of liability is correspondingly increased.

The risks that a college or university could face liability in such circumstances can be divided into three categories. First, the institution might conceivably be held responsible for the conduct of a student who introduces the virus into a computer system. Second, the institution may be held liable for the actions of its employees, including faculty members, staff, graduate students receiving financial compensation, or undergraduates employed on a part-time basis. Finally, apart from this kind of "vicarious" liability, the institution may face exposure to liability as a result of its role as a provider of computing services or for failure to use reasonable care to avoid foreseeable harm to others.

1. The University's Liability for Student Conduct

If a virus is created by a student, the college could find itself named as a defendant in a lawsuit seeking recovery for the damage caused by the virus. The student-college relationship, in and of itself, does not make a school liable for the conduct of its students: it is not a "special relationship" of the sort that obliges a person to prevent another from injuring others. Nor does one's status as a student make a person the agent of a university. See, e.g., "Tort Liability of Public Schools and Institutions of Higher Education for Injuries Caused by Acts of Fellow Students," 36 A.L.R. 3d. 330, 339 (1976). But even though the better reasoned court decisions reject the view that schools have a duty, arising from the doctrine of *in loco parentis* or otherwise, to police the private behavior of college students, some judges and juries may still find certain types of harmful activity by immature students so "foreseeable" that schools have some duty to guard against it.

As a practical matter, most colleges and universities have little choice but to bow to the realities of student independence. It is generally a poor practice for a school to promulgate a set of regulations that it will not or cannot enforce. Although having strict rules on the books may delude a school into thinking that it thereby has a responsible "policy", unenforced or unenforceable rules may come back to haunt a college if a court or jury regards the rules as establishing a standard of conduct that the school itself has failed to satisfy. Thus, the school's policies should be realistic, and enforceable. Having made clear its disapproval of irresponsible computing practices by students, a college should proceed to place its primary emphasis on policies that it can require its employees and faculty to enforce, such as operational safeguards applicable to centralized college computing facilities. Nevertheless, given the serious criminal nature and potential destructive consequences of the act of launching a destructive virus, the college should consider taking strict disciplinary action (through established procedures) against any student or employee who engages in misconduct of this sort.

2. The University's Role as Employer

Under the venerable legal doctrine of *respondeat superior*, an employer is liable for the torts committed by an employee acting "within the scope of his or her employment." Obviously, no college or university would approve, or authorize, the launching of a computer virus by any of its employees. However, the relevant test for determining whether actions are taken within the scope of employment is not whether the specific wrongful actions were included within the employee's job description, but whether, considering all of the surrounding facts and circumstances, (a) they were of the kind which the employee has been hired to perform, (b) they occurred substantially within the authorized limits of time and space, and (c) the overall conduct was, to some degree, intended to benefit the employer. On the other hand, if the employee steps outside of the employment relation to do some act for himself, unconnected with the employer's business -- engages in a "frolic and detour" -- the employer is generally not liable to injured third parties unless the employer was negligent in hiring the employee in the first place.

Although these principles are notoriously difficult to apply in any given case, a college might be held responsible for the negligence of a staff member (or a student, working part time) in promulgating a program known to contain a computer virus if the employee's job involved distributing the program to others or supervising the network on which the virus spread. Distribution of computer programs would be a foreseeable element of the job and the college, as the employer, could be held responsible for the carelessness of its agents. In contrast, the mere fact that a faculty member is employed as an instructor in computer-related subjects should not by itself expose the college to liability for independent and unauthorized acts, were such a faculty member to develop and distribute a computer virus, even with the use of college facilities.

3. The University as a Provider of Computing Services

As in all of its affairs, the college has an independent obligation to use reasonable care to protect others from foreseeable harm. Even if the

perpetrator of a computer virus were someone for whose acts the college could not be held vicariously responsible, a college might still be found liable on the ground that, in its role as operator of a computer system or network, it failed to use due care to prevent foreseeable damage, to warn of potential dangers, or to take reasonable steps to limit or control the damage once the dangers were realized. The nature of the "care" that should be deemed to be "due" in this context has not been established by statute or by judicial decision. However, the policies and actions discussed below, applied to the extent consistent with the college's other objectives, could help to prove that the college acted reasonably to minimize the risks to which others are exposed.

As a practical matter, the steps that a college takes to protect itself from disruption by viruses are likely to help minimize exposure to liability to third parties as well. The best way to reduce such risks is to establish policies that will eliminate unnecessary exposure and provide maximum preparation to deal with the emergencies that, unfortunately, seem likely to occur.

C. **Contractual Implications.**

Many colleges enter into contracts for the performance of research and for the provision of certain facilities, including computer facilities, to third parties. If a computer virus disrupts the work being performed at a college, it may cause the college or its faculty to default on the performance of various contracts -- a default that might or might not be excused by the applicable "force majeure" clauses. The level of security against the threat of viruses on a particular university computer system may have implications for the availability to the institution of certain governmental contracts or of access by its faculty to government computer systems. In addition, the college itself may be a primary provider of computing and communications services to those in the academic community. As such, it owes various contractual duties to the participants, which may include duties to take steps to reduce the risks associated with computer viruses. Finally, as both a producer and consumer of computer software, the college is continually called upon to consider the computer virus threat in entering into various software licensing

agreements.

D. Statutory Duties Relating to Privacy.

Many colleges act as providers of electronic communications services and as providers of remote computing service to the academic community. As a result of the recent enactment of the Electronic Communications Privacy Act, colleges and universities are under special duties not to disclose private electronic mail or personal storage files without proper authority. These restrictions provide for certain limited means by which governmental authorities may obtain access to computer files. Unauthorized disclosure can lead to civil liability.

III. Discussion of Specific Policies and Options

Against this background, each college should consider what combination of policies, technical protective actions, and contingency plans will best suit its needs. Consideration of these issues in advance of an actual, serious computer virus problem will help to make sure that the actions taken in the face of an emergency are effective and that the college will be found to have fulfilled its responsibilities to all concerned. Full consultation with the faculty is, of course, important to the development of sound guidelines. The following list of policy choices and action options is not meant to be all-inclusive. But it should serve to encourage discussion and to bring available alternatives into focus.

A. Establishment of Policies Regarding Student and Faculty Conduct.

In controlled circumstances, inquiries into the functioning of self-replicating computer code is a legitimate academic inquiry. Indeed, the academic community is likely to be a leading source of solutions to the computer virus problems that do exist. The primary problem is discouraging malicious or reckless behavior by those seeking glamour, thrills or publicity from launching computer viruses, in part by making clear that there is nothing admirable about taking risks with the security of the computer files that belong to others.

There are limits, as noted, on the extent of any college's role as a regulator of the conduct of its students. An unenforceable and overbroad policy may do more harm than good. But a college may choose to incorporate into its regular codes of conduct provisions that make clear that intentional disruption of computer systems is both a serious criminal offense and an ethical outrage, in view of its potential for destruction of research files and other records.

In appropriate circumstances, the college could make clear that it is the responsibility of those using college computing resources to remain vigilant for signs of improper activity and to report these immediately. Insofar as members of the university community distribute software to others, they should be urged to use special care to assure that the disks they distribute are free of any destructive code, from whatever source. Reckless experimentation with computer viruses -- not undertaken in carefully controlled circumstances -- could appropriately be made grounds for stern disciplinary action.

Clearly stated policies of this sort will help to prevent problems and to support arguments that the college should not be found liable for destructive actions taken by an individual student or faculty member.

B. Distribution of Information.

Much ignorance remains regarding the nature of the threat posed by computer viruses. Many students may not appreciate the fact that they face significant risks if they exchange unauthorized copies of pirated software. Some computer users may not be aware of their option to install software that monitors their computer system for actions that might be taken by computer viruses. Many users of computer networks fail fully to appreciate the importance of protecting their passwords.

Education about the nature of viruses, and about what to do when a computer virus hits, can help to limit the problem. Care should be taken not to dispense so much information on this subject as to increase interest in it, educate would-be perpetrators, or feed rumor mills regarding the extent of the actual threat. But a calm educational campaign could help members of

the academic community to avoid and to spot trouble -- and would help the college to prove that it exercised due care in its efforts to avoid any problems. In particular, a college might choose to make sure that all computer users and staff are told who to call in case of an emergency, are instructed in sound backup practices, are made aware of typical virus symptoms, can easily identify and obtain virus protection programs, and are told what sources of software are relatively more reliable than others.

C. **Limitations on Access to College Computers.**

Where the college controls access to a computer network or a computer center, it may want to consider imposing more stringent controls over access to such computers. Some options include:

- requiring passwords for access to the system;
- "bouncing" would-be users after they supply a few invalid passwords, and recording all such unsuccessful access attempts;
- requiring proof of affiliation with the college as a condition for access to a campus computing center;
- keeping detailed records of who has had access to particular machines at particular times;
- limiting computer access by terminated employees or students who have been subjected to disciplinary action;
- prohibiting or restricting the loading onto college networks of certain types of high-risk software programs, such as "shareware", public domain software, and programs recently downloaded from small, privately run bulletin boards;
- requiring a showing of need before allowing any student or staff member to access system software on multiuser systems;
- requiring staff to devote greater attention to monitoring the use of campus computer systems and to checking for evidence of unusual or suspicious activity.

Staff with responsibility for the college's computer systems should be centrally involved in analyzing these or other protective policies, and should be

given necessary resources to carry out these functions.

D. **Establishment of Operational Safeguards.**

A college might take a number of steps, in addition to establishing access restrictions, to reduce the risks of harm from a computer virus:

•installing software programs that keep watch for computer viruses (e.g., by checking file sizes and looking for programs that alter files unexpectedly);

• distributing only software licensed from known, reputable commercial sources;

• installing PC software at college computing centers directly from shrinkwrap packages, with a locked copy of the original disk kept in storage off site;

• testing high-risk software such as "shareware" and public domain software;

• initially installing new software of uncertain origin on an isolated computer system;

• encouraging the use of "write protect" tabs on program disks;

• immediately investigating unexplained or suspicious activity, including unauthorized attempts to achieve remote access or to alter files;

• immediately removing from the college's computers any software that exhibits symptoms of possible virus infection;

• establishing backup policies designed to assure that clean copies of uninfected application programs remain available for a reasonable time;

• requiring the grandfathered rotation of backup copies, stored off site;

• conducting periodic security audits to determine whether reasonable steps have been taken to assess and counter the virus threat in light of the particular circumstances facing the college.

E. **Creation of an Emergency Action Plan.**

A college may want to establish an emergency action plan to help reduce the impact of any computer virus problems that its preventive measures do not eliminate. Such a plan might include some of the following elements:

• collecting a list of the college staff and facilities that need to be notified immediately in the event of a problem;

• compiling names and phone numbers of outside computer experts who can be called on short notice to help in response to an emergency;

• appointing one staff member to coordinate the college's response to a computer virus emergency.

Any plan adopted by the college should be the subject of periodic review and practice sessions, to help assure that major problems have been anticipated in the plan.

F. Development of Plans for Response to Governmental Inquiries.

If a serious incident occurs, it is possible that the police (or, indeed, FBI) may become involved. Colleges need to plan to be able to respond quickly and helpfully to governmental inquiries without violating the rights of students or faculty members. In order to obtain access to the contents of private messages or files on a college computer system, law enforcement officials will usually need a warrant or a grand jury subpoena. Access to certain other types of records regarding activity on the college computer system may not require such authorization. Because the police may not know who committed the offense, they may seek unreasonably broad access to the college's computer systems and to files the college maintains on behalf of others. Before granting such access, the college should seek legal counsel.

G. Review of Contractual Rights and Obligations.

As a consumer and provider of computer software and systems, a college has many different contractual relationships. These should be reviewed with a view to the new dangers and duties posed by computer viruses. For example, if the college computer network is provided by a third party vendor, the contract between the college and the vendor should call for the vendor to cooperate fully with the college in implementing appropriate protective policies. Insofar as the college provides software or services to others under contract, it should limit its warranties and liability, as is the industry practice. But if the college becomes aware that a computer virus is

contained in any software it has provided to others, it should carefully consider whether it has a duty promptly to inform known recipients of the danger and to take other reasonable steps to assist in eradicating the problem. The college might decide to include in its future contracts a provision that the college's obligations would be excused or deferred in the event of disruption by a virus. A college should review its insurance coverage, with an eye both to protection against the costs of recovering from a virus attack and to protection against liability to others for the actions of its students and employees.

IV. Conclusion

The threats posed by computer viruses are sufficiently new that few laws specifically address them, and no court decisions delineate the actions a college has a duty to take to deal with these threats. Yet the risks posed by computer viruses may be greatest in the academic community. The best protection available -- against both damaging incidents and legal liability -- is to give careful thought to the adoption of a reasonable set of protective policies compatible with other institutional goals. While some of the issues are technical in nature, many sources of technical assistance are available. Policy choices will involve a need for balancing concerns about the computer virus threat against equally valid concerns that protective measures not interfere with productive use of computers as exciting educational and research tools. Each institution, in a manner suited to its own circumstances, should be able to demonstrate that it has planned in a thoughtful and measured way to reduce the risk without unduly interfering with legitimate educational objectives.

Published by

Two Wisconsin Circle
Suite 1040
Chevy Chase, Maryland 20815-9913

Telephone (301) 907-4908
(800) 346-7877

United Educators Insurance Risk Retention Group, Inc.
Two Wisconsin Circle
Suite 1040
Chevy Chase, Maryland 20815-9913